# Governance and Management

Updates to this material are, in part, either adapted or excerpted from *Software Security Engineering: A Guide for Project Managers* [Allen 2008[1]].

## Description

Governance and management of security are most effective when they are systemic, woven into the culture and fabric of organizational behaviors and actions. In this regard, culture is defined as the predominating shared attitudes, values, goals, behaviors, and practices that characterize the functioning of a group or organization. Culture thereby creates and sustains connections among principles, policies, processes, products, people, and performance. Effective security should be thought of as an attribute or characteristic of an organization or a project. It becomes evident when everyone proactively carries out their roles and responsibilities, creating a culture of security that displaces ignorance and apathy. One manifestation of this is that everyone proactively considers the attacker perspective throughout the software development life cycle and how the software can fail when under intentional attack or unintentional actions of users or developers.

This means that security must come off the technical sidelines as activities and responsibilities solely relegated to software development and IT departments. Today, boards of directors, senior executives, and managers all must work to establish and reinforce a relentless drive toward effective enterprise, information, system, and software security. If the responsibility for these is assigned to roles that lack the authority, accountability, and resources to implement and enforce them, the desired level of security will not be articulated, achieved, or sustained. Contrary to the popular belief that security is a technical issue, even the best efforts to buy secure software and build security into developed software and operational systems encounter "considerable resistance because the problem is mostly organizational and cultural, not technical" [Steven 2006][2]. Software and information security are about spending money, with the measure of success being that nothing bad happens. As time goes on, this can become a tough sell to business leaders as the “we haven't been attacked lately so we can cut back on spending” mentality sets in.

Project managers need to elevate software security from a standalone technical concern to an enterprise issue when both developing and acquiring software. Because security is now a business problem, the organization must activate, coordinate, deploy, and direct many of its core resources and competencies to manage security risks in concert with the entity’s strategic goals, operational criteria, compliance requirements, and technical system architecture. Those responsible for ensuring secure software should have the responsibility and authority to stop the release of new software into production if security requirements are not met.
To sustain enterprise security, the organization must move toward a security management process that is strategic, systematic, and repeatable, with efficient use of resources and effective, consistent achievement of goals [Caralli 2004b][3].

The objective of this content area is to help software developers and their managers, and security professionals and their managers: (1) more effectively engage their leaders and executives in security governance and management by understanding how to place information and software security in a business context and (2) better understand how to enhance current management practices to produce more secure software. Armed with this material, managers and developers can build attentive, security-conscious leaders who are in a better position to make well-informed security investment decisions. With this support, they can then take actionable steps to implement effective security governance and management practices across the software and system development life cycle.

[1] http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/management/564-BSI.html#dsy564-BSI_allen2008 (Governance and Management References)

[2] http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/management/564-BSI.html#dsy564-BSI_wp1012350 (Governance and Management References)

[3] http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/management/564-BSI.html#dsy564-BSI_wp1012153 (Governance and Management References)

## Articles in this Content Area

The articles in this content area provide a recommended order of steps to tackle to govern and manage enterprise, information, and software security.

1. The overview, "Security Is Not Just a Technical Issue[4]," defines the scope of governance concern as it applies to security. It describes some of the top-level considerations and characteristics to use as indicators of a security conscious culture and whether an effective program is in place.
2. The second article, "How Much Security Is Enough?[5]," provides guidelines for answering this question, including strategy questions to ask, organizational and market characteristics to take into account, and means for determining adequate security based on risk. It is important to make sure that leaders understand the residual risk that remains after mitigating actions are taken.
3. The third article, "Maturity of Practice[6]," identifies several indicators that organizations are addressing security as a governance and management concern, at the enterprise level. It summarizes how some organizations, trade associations, and market sectors are proceeding. Many of the references and links in this article provide more detailed implementation guidance.
4. The fourth article, "Adopting an Enterprise Security Framework[7]," by John Steven, originally appeared in *IEEE Security & Privacy*. It describes a suggested approach for putting an enterprise-wide software security program in place, including necessary governance and management actions. According to Steven, "Put simply, without executive sponsorship, a unified understanding of roles, responsibilities, and a vision for software security, the effort will sink quickly into political struggle or inaction."
5. The fifth article, "Making Business-Based Security Investment Decisions – A Dashboard Approach[8]," presents an approach for selecting security investments using business-based criteria. The approach and supporting tool define seven decision criteria categories, each supported by three or more indicators. Categories and indicators are ranked and applied to a series of investments. Individual investment scores are presented for discussion and evaluation by decision makers.

Articles 1, 2, 3, and 5 draw from a wide range of technical reports, other materials, external sources, and collaborators who are successfully addressing this topic. They summarize CERT field work and applied research conducted over the past two years. Much of this content draws from and is expanded in [Allen 2005][9] and [Westby 2007[10]].

## Notes to the Reader

The articles in this content area

- address security at the enterprise and organizational level, *not* at the system or software level, although examples at this level are provided. CERT research and field experience indicate that enterprise-level action is necessary to achieve and sustain secure systems and software and protect the security of information. This includes the commitment and action to address security throughout the software development life cycle.
- are written for security professionals and their managers, seeking to more effectively engage their leaders and executives in security governance and management
- intentionally do not clearly distinguish between security governance and security management. Typically, governance is responsible for direction, control, and oversight, and management is responsible for execution. The roles and distinctions vary widely by type of organization and the market sector within which an organization operates.
- do not provide detailed "how-to" guidance. The third and fourth articles provide exemplars and frameworks to consider. Articles in other BSI content areas provide more details to help enact the recommendations presented here. These include Acquisition[11], Architectural Risk Analysis[12], Assembly,

[9] http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/management/564-BSI.html#dsy564-BSI_wp1012117 (Governance and Management References)

[10] http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/management/564-BSI.html#dsy564-BSI_Westby07 (Governance and Management References)

Integration, and Evolution[13], Business Case Models[14], Incident Management[15], Measurement[16], Principles[17], Project Management[18], Risk Management[19], and SDLC Process[20].

## Podcasts on Enterprise Security

"Security for Business Leaders[21]" is a series of conversations that provide both general principles and specific starting points for business leaders who want to launch an enterprise-wide security effort or make sure their existing security program is as good as it can be. Podcasts under the heading "Software Security[22]" are particularly relevant.

## Overview Articles

| Name | Version Creation Time | Abstract |
|---|---|---|
| Security Is Not Just a Technical Issue | 11/30/09 12:47:57 PM | Updates to this material are, in part, either adapted or excerpted from *Software Security Engineering: A Guide for Project Managers* [Allen 2008[23]].<br>This overview defines the scope of governance concern as it applies to security. It describes some of the top-level considerations and characteristics to use as indicators of a security conscious culture and whether an effective program is in place. |

## Most Recently Updated Articles [Ordered by Last Modified Date]

| Name | Version Creation Time | Abstract |
|---|---|---|
| Governance and Management References | 12/1/09 3:03:32 PM | Content area bibliography. |
| Security Is Not Just a Technical Issue | 11/30/09 12:47:57 PM | Updates to this material are, in part, either adapted or excerpted from *Software Security Engineering: A Guide for Project Managers* [Allen 2008[24]].<br>This overview defines the scope of governance concern as it applies to security. It describes some of the top-level considerations and characteristics to use as indicators of a security conscious culture and whether an effective program is in place. |
| Maturity of Practice | 11/30/09 11:41:13 AM | Updates to this material are, in part, either adapted or |

[21] http://www.cert.org/podcast/

[22] http://www.cert.org/podcast/#softsecurity

| | | |
|---|---|---|
| | | excerpted from Software Security Engineering: A Guide for Project Managers [Allen 2008][25].<br>This article identifies several indicators that organizations are addressing security as a governance and management concern, at the enterprise level. It summarizes how some organizations, trade associations, and market sectors are proceeding. Many of the references and links in this article provide more detailed implementation guidance. |
| How Much Security Is Enough? | 11/30/09 11:16:54 AM | Updates to this material are, in part, either adapted or excerpted from Software Security Engineering: A Guide for Project Managers [Allen 2008][26].<br>This article provides guidelines for answering this question, including strategy questions to ask, organizational and market characteristics to take into account, and means for determining adequate security based on risk. It is important to make sure that leaders understand the residual risk that remains after mitigating actions are taken. |
| Framing Security as a Governance and Management Concern: Risks and Opportunities | 11/14/08 2:50:48 PM | This article briefly describes six "assets" or requirements of being in business that can be compromised by insufficient security investment. Conversely, adequate security investment can reduce risk and create business opportunity. The article closes by describing barriers that must be overcome when forming security governance and management programs. |

## All Articles [Ordered by Title]

| Name | Version Creation Time | Abstract |
|---|---|---|
| Framing Security as a Governance and Management Concern: Risks and Opportunities | 11/14/08 2:50:48 PM | This article briefly describes six "assets" or requirements of being in business that can be compromised by insufficient security investment. Conversely, |

| | | |
|---|---|---|
| | | adequate security investment can reduce risk and create business opportunity. The article closes by describing barriers that must be overcome when forming security governance and management programs. |
| Governance and Management References | 12/1/09 3:03:32 PM | Content area bibliography. |
| How Much Security Is Enough? | 11/30/09 11:16:54 AM | Updates to this material are, in part, either adapted or excerpted from Software Security Engineering: A Guide for Project Managers [Allen 2008][27].<br>This article provides guidelines for answering this question, including strategy questions to ask, organizational and market characteristics to take into account, and means for determining adequate security based on risk. It is important to make sure that leaders understand the residual risk that remains after mitigating actions are taken. |
| Making Business-Based Security Investment Decisions – A Dashboard Approach | 10/22/08 6:04:24 PM | This article presents one approach for selecting security investments using business-based criteria. The approach and supporting tool define seven decision criteria categories, each supported by three or more indicators. Categories and indicators are ranked and applied to a series of investments. Individual investment scores are presented for discussion and evaluation by decision makers. Our intent is that this approach can be use to rationalize and prioritize any class of security investments including software assurance. |
| Maturity of Practice | 11/30/09 11:41:13 AM | Updates to this material are, in part, either adapted or excerpted from Software Security Engineering: A Guide for Project Managers [Allen 2008][28].<br>This article identifies several indicators that organizations are addressing security as a governance and management |

|  |  |  |
|---|---|---|
|  |  | concern, at the enterprise level. It summarizes how some organizations, trade associations, and market sectors are proceeding. Many of the references and links in this article provide more detailed implementation guidance. |
| Security Is Not Just a Technical Issue | 11/30/09 12:47:57 PM | Updates to this material are, in part, either adapted or excerpted from *Software Security Engineering: A Guide for Project Managers* [Allen 2008[29]].<br>This overview defines the scope of governance concern as it applies to security. It describes some of the top-level considerations and characteristics to use as indicators of a security conscious culture and whether an effective program is in place. |